State of Nebraska

Computer Network External Intrusion Security Assessment

Summary of Findings and Recommendations

August 2003

Compiled By The
Office of the Chief Information Officer
State of Nebraska
521 South 14th Street, Suite 200
Lincoln, Nebraska 68506

402.471.4385
www.nitc.state.ne.us

TABLE OF CONTENTS

BACKGROUND

The Nebraska Information Technology Commission (NITC) Security Policies (http://www.nitc.state.ne.us/standards/index.html) require an annual audit of network security. Federal regulations that govern several critical state programs also require security assessments. Independent security assessments are widely considered to be sound business practice in the information technology security field.

To begin addressing this need, the NITC awarded a grant to conduct an external intrusion security assessment of the state's network. Following a careful process to develop an RFP and select a qualified vendor, the Chief Information Officer in January 2003 awarded a contract to Omni Tech Corporation (omnitechcorp.com). The security assessment focused on Internet vulnerabilities, only. It did not involve an on-site review of security policies, interviews, evaluation of network configurations, or a test of security systems, which are elements of other types of security assessments and audits.

The project consisted of three phases. The goal of the Discovery Phase (Phase I) was to perform intelligence gathering and foot printing activities. The Scan Phase (Phase II) identified known vulnerabilities across the entire network. The Test Phase (Phase III) provided highly skilled analysis and attacks against a limited number of state agencies. A high priority of all three phases was to avoid any disruption of services.

Several activities were outside the scope of this engagement. These included war dialing, wireless security assessment, security testing of business applications, and social engineering.

This report presents the findings and recommendations from the external intrusion security assessment. It is based on the detailed technical reports submitted by Omni Tech following each of the phases. Also, on July 29, the CIO met in Milwaukee with the entire team assigned to this project. That briefing provided additional insights and suggestions for improving security of the state's network.

In computer security there are always opportunities for improvement. The purpose of this security assessment was to provide insight into existing vulnerabilities and help promote better security practices. The most important finding of this engagement was the active interest in security issues on the part of the technical staffs in many agencies.

Other Security Initiatives. The external intrusion security assessment is just one part of a long term and continuing effort to address computer security issues. Over the last three years, we have developed a comprehensive set of security policies, prepared handbooks for security officers to use in preparing security programs, and written a security incident reporting procedure. We held a Security Awareness Day on July 15, 2002, and made available a security awareness training application. Recently, the NITC adopted a set of guidelines for disaster recovery planning. Work will commence, soon, on a template for business continuity planning for state agencies. A security work group recently completed policies and guidelines pertaining to remote access and wireless security, which will be presented to the NITC for review and approval in September. More information is available at: http://www.nitc.state.ne.us/tp/workgroups/security/index.htm.

SUMMARY OF METHODOLOGY, FINDINGS AND RECOMMENDATIONS

PHASE I -- DISCOVERY

Methodology

Omni Tech Corporation performed the Phase I section of the assessment project against the State of Nebraska's registered Class B address range of 164.119.x.x. The purpose of Phase I was to identify the accessible systems from the Internet and to do preliminary footprinting of those systems. Several tools were used to do initial discovery of the State's Internet presence, including but not limited to; ARIN, NMAP, SecureScan NX, Telnet, ping, and nslookup. Also, the IP range's registration was verified using the Whois database.

Omni Tech Corporation discovered 1,545 hosts that responded in one way or the other to its tools. The number of discovered devices indicated the expected configuration of most hosts being filtered from the Internet by firewalls and other perimeter devices.

Phase I also involved scanning for open ports. There are a possible 65,535 ports on every system. These ports can be associated with services that can be accessed from the Internet. HTTP, for example, is a common service used by web pages. The "standard" port for HTTP is port #80. This process involves attempting to make a connection with the host on a number of ports. During Phase I, Omni Tech Corporation scanned ports 1-1024, 1080, 1433, 3100, 3389, 5900, 8000, and 8080. The decision was made to scan a limited number of ports to minimize the possibility of interruption of services. In Phase II and III more aggressive scanning may be performed to further interrogate systems for "non-standard" configurations.

During the initial phases no Intrusion Detection Systems (IDS) were observed. No active searches were made for IDS systems and the network discovery went as anticipated. A typical indication of an IDS system would be loss of connectivity to systems in a range of IP addresses protected by such a system. Typically IDS or shunning firewalls can be configured to ignore traffic from devices suspected of hacker-like activity (usually port scanning).

A sampling of mail servers was checked against several "blacklist" servers for spam relay identification. Blacklists are services, which identify known or suspected offenders of email abuse. Many mail systems rely on these lists to identify spammers and block email from these addresses. None of the IP addresses tested was identified as spam relays.

Findings and recommendations of Phase I include:

1. Turn off "ping" at the firewall, because responding to a ping makes it too easy for a hacker to conduct a discovery sweep.

2. Some of these devices are configured to respond to a port scan with a reset, as opposed to a timeout (the preferred configuration from a network security perspective). While this is not a risk per-se it does indicate a possible configuration issue that should be investigated. The more work an intruder has to do to map a network the better. If a host responds with a reset it is a definite indication that a host exists and more investigation is warranted. If a port scan times out, it takes much longer and leaves doubt to whether a host is there or not.
3. The number of devices configured to the Internet is probably too large. PCs, printers, copiers, and other devices should not be configured to the Internet. In general, the only hosts that should be configured to the Internet are those needed for serving content.
4. Numerous hosts were discovered to have unneeded services running that could indicate vulnerable systems. These unneeded services should be turned off, because they give the potential hacker too much information, and there is always the potential for new vulnerabilities targeted to a particular service. Options include blocking everything at the firewall at the perimeter AND turning the services off at the host level. Outdated or non-standard configurations were also noted, and several services were discovered running on non-standard ports, which could indicate a security issue or an improper configuration. These unneeded services are listed in Appendix A.
5. Consider Intrusion Detection System (IDS), AFTER the range of targets is narrowed. Fix network holes first, otherwise the volume of IDS alerts is unmanageable. Use IDS on the inside of the firewall to record events that should not have happened. Configure the IDS to watch for specific things on specific servers.

PHASE II -- VULNERABILITY SCAN

Methodology

Omni Tech Corporation conducted a limited scan using automated tools such as Retina, Nessus, and SecureScanNX. "Limited" means that any known-to-be-dangerous tests were not used. In addition, Omni Tech Corporation managed both the depth and aggressiveness of the scans to minimize the risk of disruption.

The decision was made that Phase II targets would be broken up along Class C lines for easier report dissemination by agency and to distribute the traffic on the State's network. These guidelines were followed with the exception of the 164.119.9.x and 164.119.10.x networks, which are not "assigned" to an individual agency, but are broken up into many agencies. The .9 and .10 subnets were broken out by agencies, as identified by the Division of Communications and Information Management Services Division.

Any scanning tool will miss certain vulnerabilities. These "false negatives" may result from something as simple as a service not being available at the time of the scan. Additionally, it may be because of the conservative settings chosen to prevent the risk of service disruption. Any scanning tool will report vulnerabilities, which do not actually exist. These "false positives" may result from something as simple as a service that provides misleading version information. If a host in Phase II is identified with a vulnerability, manual verification may be necessary to verify the accuracy of the report.

Out of 1545 hosts identified in phase I, a total of 2765 vulnerabilities were found. 139 hosts are likely to contain “high risk” vulnerabilities, 1186 are likely to be susceptible to “medium risk” vulnerabilities and 1429 may contain “low risk” vulnerabilities. These figures represent the total number of incidents in each category of risk. Many hosts had multiple vulnerabilities. Three agencies had no high or medium risk vulnerabilities. Agencies that do not address network vulnerabilities pose a threat to other agencies on the network and to agencies that share services.

Omni Tech defines “high risk vulnerabilities” as a flaw in the system or configuration, which by itself may give an attacker direct access to manipulate information. Medium risk is defined as a flaw in the system or configuration which, when combined with other vulnerabilities or information, may provide access to information. Low risk is considered a vulnerability that discloses configuration information about a host. The information provided is not required for the application to function and provides an attacker with unnecessary “target definition” data.

Overall risk also depends on whether a system is critical and whether multiple risks exist that magnify the potential for problems. Combining several lower risk vulnerabilities on a server with "interesting" data may create sufficient incentive and enough holes for a hacker to compromise the system. The ability to compromise one server on the network and use it as a base of operations to attack other servers on the network can also magnify the significance of vulnerabilities on the target server.

Phase II confirmed the finding of too many hosts and too many open ports and services exposed to the Internet. This problem was widespread but especially serious in a few agencies. Appendix B lists some of the more critical vulnerabilities.

During the course of defining the targets for Phase II, it was discovered that there is no “centralized” authority for the identification of IP addresses assigned to State agencies. This became very problematic when it came time to identify the targets of the vulnerability scan, as it was the State’s desire to have individual reports for each agency. Several lists were provided to identify the mappings of IP address to hosts belonging to State agencies, but these lists were out of date and inaccurate. At the conclusion of Phase II it is unreasonable to assume that the targets addressed by the scans are inclusive of each State agency. Some systems surely have been overlooked.

Findings and recommendations of Phase II include:

1. There are too many hosts, open ports and unneeded services exposed to the Internet. This gives potential hackers too much information and there is always the potential for new vulnerabilities targeted to particular services. The state should adopt a stringent test for opening a port and services: "what is the compelling reason for the service?" If a compelling case does not exist, the default should be to shut off the port and service.
2. Complete and accurate information on the assignment of IP addresses does not seem to exist. Network maps and network diagrams are important tools for managing networks, including understanding what systems are critical, determining network configuration, and responding to problems. Require IP registration of all devices configured on the network. Information should include the IP address, type and function of the device, agency, and contact person. A network map and diagram should show the connections of all devices and identify what assets need the highest levels of protection. Registration should start with a high-level, simple database that focuses on mission critical devices.

3. A significant number of potential vulnerabilities exist. It is important to eliminate existing vulnerabilities. This should include:
   3.1. Address high risk vulnerabilities at the host level;
   3.2. Configure the firewall to restrict traffic for some services to a specific host, if there is a valid reason to keep that service open.
   3.3. Focus on the total number of open services and vulnerabilities as the measure of progress, not just high-risk vulnerabilities.
4. The State should establish an expectation that vulnerabilities should be an aberration. There should be a continuous effort to identify and eliminate vulnerabilities now and in the future. The strategy should include keeping patches current and adopting sophisticated firewall management, including an application firewall in some situations.

PHASE III – TESTING AND VERIFICATION

Methodology

Omni Tech Corporation performed Phase III of the security assessment project for the purposes of testing and verification. Phase III also served to demonstrate the potential consequences associated with vulnerabilities. Pursuant to the terms of the engagement, testing and verification focused on a subset of agencies. The CIO identified 19 agencies for inclusion in Phase III, based on several criteria: number of vulnerabilities, agency desire, and risk profile of the agency. Omni Tech Corporation determined which servers to attack in each agency, based on vulnerabilities and apparent value of the asset.

Omni Tech Corporation analyzed the results of Phase II as a starting point for Phase III. High and medium risk vulnerabilities were analyzed for suitability for exploitation. Phase III also investigated the possibility of exploiting other available services that Phase II did not initially identify as being subject to attack. Exploits may exist for some of these services, or they may provide information about the target that can be used by a hacker in other ways.

The actual number of hosts tested was reduced based on the availability of vulnerabilities and the functionality of the host. While the primary target may have been a high profile host, such as a Web server, the possibility of exploiting lesser hosts that may lead to more important hosts was also investigated.

Omni Tech Corporation conducted Phase III with significant constraints to avoid any disruption of service. Constraints included taking no action that would crash a system, only using tools that have been proven to be safe, not engaging in destructive testing, not mounting denial of service attacks, and not modifying nor deleting data. As conducted, Phase III activities represent the initial research for a full penetration attack or social engineering.

Omni Tech Corporation combined the results of individual scans for each agency participating in Phase III to generate an agency view of vulnerabilities discovered, available services, and open ports. The methodology then used the following steps:

1. Target selection was based on the Phase II results.
   1.1. High and medium risk vulnerabilities detected.
   1.2. Web servers with the potential for interesting data.

2. Manual verification of High and Medium risk vulnerabilities.
   2.1. Verified through extended data on Phase II report. (Extended data is the information returned by the scanning tool as a result of a test case being run; e.g., banner information from a web server that identifies its version.)
   2.2. Verified using a separate tool. (Telnet, GetIF, Browser, etc.)
   2.3. Not all vulnerabilities could be verified without an exploit or crashing the host.
   2.4. Tools used during testing were limited to trusted sources. In the case of open source tools, source code was analyzed to prevent any unknown additional effects such as Trojans or malicious applications.
   2.5. Web server source code was analyzed to provide information regarding the web applications running on a server, i.e., Cold Fusion, Active Scripting Pages, CGI scripts.

The scope of the project for the State of Nebraska was that of an assessment. The project did not include a penetration test which would have taken all the data thus far and investigated the possibility of compromising hosts on the inside of the State's network. Much of the data collected and vulnerabilities discovered would have provided many opportunities to compromise more of the State's network. Several hosts revealed valuable data for social engineering, which is often a component of penetration testing.

Findings and recommendations of Phase III include:

1. Three servers were compromised to the point of ownership (owned in hacker terms) meaning the ability to perform any functions desired on the device. These are most probably not the only hosts subject to compromise. There were many other vulnerable hosts that have exploits which are either not available (unpublished) or could not be found. We felt that this does not make the host secure, it merely means that given the scope of the project we where not able to exploit the vulnerabilities.
2. Fifty-five vulnerabilities were verified in the 19 agencies tested. These do not include low risk vulnerabilities, which are typically banner (informational only) or simple TCP services (which were detailed in Phase I).
3. A noticeable number of vulnerabilities have been addressed by some agencies. By verifying the Phase II results we were able to determine that several vulnerabilities have been addressed.
4. While the majority of the vulnerabilities were unable to be exploited, this does not mean that a problem does not exist. A determined intruder could still potentially exploit these issues by using tactics or exploits that Omni Tech Corporation could not use under the terms of the engagement. The important thing to keep in mind is that every hole (vulnerability, service, application) provides an intruder with another way into the network. Even low risk vulnerabilities (such as simple TCP services) can assist an intruder in attacking a network.
5. It was apparent that many agencies are not filtering traffic, which compounds the issue of extra services and out of date applications. If basic filtering were in place the majority of vulnerabilities would not have been revealed from the external network. While filtering external traffic does not resolve the vulnerability, it does reduce the risk profile from the majority of networked systems (Internet).

CONCLUSIONS

It appears that the agencies addressed many of the findings from Phase II once they received the reports. Many of the hosts had been removed from the Internet or blocked using a firewall or similar filtering device. A substantial number of vulnerable hosts still existed in agencies participating in Phase III, which reflects just a percentage of the overall hosts in Phase II.

We believe that this project has raised awareness in the State to the existing issues that could lead to compromised information on the network. Such compromises may have already occurred. The best way to assure no further compromises would be to follow the "least privileged" mode of operations. Multiple layers of filtering would also prevent any compromise from spreading into other departments.

Further testing on the hosts that have been identified as vulnerable should be performed to insure that the identified vulnerabilities no longer exist.

A procedure should be adopted to prevent future vulnerable hosts from being placed on the State's network to minimize the risks. This procedure should include documentation and testing of the latest patches and security fixes being applied before hosts are allowed on the Internet. Testing of hosts should also occur on a periodic basis to assure that no changes have been made that could open new holes on a host.

Segmentation of the State's network will help minimize the possibility of an intruder compromising one agency and moving on to other connected agencies. Firewalls or other filtering devices should be in place to separate the different agencies, providing another layer of protection from attack.

Filtering traffic at many layers would also improve the risk profile of the State's network, assuring that if an agency neglects to address an issue the filtering could take place at another layer of the State's network. Currently a majority of the host on the State's network responds to a PING request (ICMP echo). This service is not typically necessary and only assists an intruder in mapping the network. Filtering ICMP traffic would be the most effective way of reducing this exposure.

Mapping the State's network from a visual standpoint would greatly assist in designing a more secure network. Visualizing the network requires a deeper knowledge of the IP addressing scheme and also shows the possible connection points between agencies (such as shared systems).

APPENDIX A

LIST OF UNNEEDED SERVICES (PHASE I)

Services listed below are typically considered to be inappropriate for external access. The detailed report lists the host on which these services can be found.

From an information security view, it is recommended to close all ports that are unneeded to secure the system from known and unknown attacks. The following ports should be disabled if possible, or access to these ports should be controlled at the router or firewall to limit the exposure to the greatest extent.

- CableRouter: The following IP addresses may have a Linux remote desktop service running on port 1024. The PAM console module in Linux systems allows a user to access the system console and reboot the system when a display manager such as gdm or kdm has XDMCP enabled. (4 IP addresses)
- Cachefsd: The CacheFS file system is a general purpose caching mechanism that improves NFS server performance. CacheFS is a "helper service" and is not needed on the external network. (1 IP address)
- Chargen: A character generator service used for troubleshooting. Unnecessary service that can be used to attack systems. (43 IP addresses)
- Daytime: A service that provides the current time. The service can be exploited to cause a "denial of service" attack. Typically not used. (42 IP addresses)
- Discard: The discard service basically throws away any data sent to it. There is no practical use for this service. (51 IP addresses)
- Echo: As the name implies, any data sent to this port is "echoed" back to the requestor. This service can be used for "denial of service" attacks and should be disabled. (58 IP addresses)
- Epmap: End-point mapper helper service typically used for LAN-based Windows networking. (118 IP addresses)
- Famrpc: RPC helper service with no valid use. Should be disabled. (1 IP address)
- Finger: A simple service that can remotely identify users who are logged in. (36 IP addresses)
- Gopher: A predecessor to HTTP. This service is outdated and no longer used. (8 IP addresses)
- LanMan: Windows LAN Manager service. An outdated security service, which should be upgraded to a more secure mechanism. (95 IP addresses)
- Mountd: Daemon used to "mount" or map drives on remote systems. This service is highly insecure and can be easily tricked. (4 IP addresses)
- Ms-sql-s: SQL database service provides direct access to the database and should not be available to the Internet. (32 IP addresses)
- NetBios Name: The Netbios service should not be made available to the Internet, because it discloses information about systems. (7 IP addresses)
- NetBios Session: The NetBios service should not be made available to the Internet, because it discloses information about systems. (97 IP addresses)
- Nfs: The Network File System (NFS) is a client/server application that lets a computer user view and optionally store and update files on a remote computer as though they were

on the user's own computer. NFS has known insecurities and should not be used on the public network (2 IP addresses)

- Nlockmngr: An NFS helper service used to lock volumes. Should be disabled along with NFS. (4 IP addresses)
- Pop2: Post Office Protocol 2 is a simple mail protocol not typically recommended due to the weak authentication mechanism. (1 IP address)
- Pop3: Post Office Protocol 3 is a simple mail protocol not typically recommended due to the weak authentication mechanism. (39 IP addresses)
- PortMapper: This service "advertises" the other services available from this host. It should be blocked from the outside. (19 IP addresses)
- Printerd: (Printer ports found) The following list of IP addresses was found to have a printer configured. It is not typically expected to see printers on the outside of the network. This may indicate a configuration issue with a filtering device or the placement of the device may be insecure. (36 IP addresses)
- Quote (quote and rquotad): Quote of the day service, sends a short message to clients when they login. There is no production value in this service. (31 IP addresses)
- Rlogin and rsh: R-services or remote services are insecure protocols and should not be used. There are acceptable replacements for these services that provide the same functionality securely. (11 IP addresses)
- RTSP: Real time streaming player. This could be a legitimate server for serving up real time video or audio. (1 IP address)
- Remote Access (Timbuktu, VNC Server, and Windows_TerminalServer4): Several ports were identified which could potentially be used to remotely access machine and take over full control. These types of services are not generally recommended on external facing machines due to the risk of unauthorized access. If remote access is necessary it is recommended that the traffic would be tunneled through an encrypted connection such as VPN. (88 IP addresses)

APPENDIX B

LIST OF CRITICAL VULNERABILITIES (PHASE II)

1. SNMP Available.

Simple Network Management Protocol is a service that provides read and write capabilities over a network which allows for remote management. SNMP was a "temporary" protocol developed in the earliest stages of what we now know as the Internet. The protocol was not intended to be used in production environments; therefore no real security features were designed into the protocol. All traffic travels in "clear text" meaning it can easily be intercepted and captured or manipulated. The only form of security available is known as a "community string." This is a simple password assigned by the administrator. Unfortunately, this information also travels in the clear and is easily intercepted. At a minimum all SNMP traffic (port 161 UDP) should be blocked at the perimeter of the State's network. All hosts identified should be configured with an access list of authorized hosts if SNMP is found to be necessary. Configuration of the default community strings should also be modified with a difficult to guess password to prevent the casual intruder from gaining access by luck. The service should also be configured for "read only" to prevent anyone from making changes to systems without authorization. The chart below reflects that the majority of all vulnerabilities are related to port 161, which is the default port for SNMP. The biggest impact on the number of vulnerabilities can be realized by addressing this issue.

2. Telnet and FTP

A total of 79 hosts were found to be running Telnet and 89 hosts were running FTP. These protocols are considered insecure and should be replaced by secure shell and secure copy. It was also observed that several services are running on non-standard ports, which is not a known vulnerability, but may indicate a situation where the service is unauthorized and is trying to avoid detection by running on a non-standard port. The systems running telnet on 2001, 6001, and 9001 are most likely Cisco devices. These may be configured as "reverse telnet" ports, which may allow the devices to be used as hopping points for hackers.

3. Unnecessary Ports

As we discovered in Phase I, many hosts have ports and services running that are unnecessary. These services can be used to gather information or disrupt services on systems running on the Internet. The best practice would be to remove or disable these services from the host themselves, but a temporary fix would be to restrict traffic at routers to limit traffic to approved protocols.

A large number of ports were found to be open on many systems. This indicates a larger problem with the configuration of the State's wide area network and filtering procedures. Best security practices recommend that only "authorized" traffic should be allowed to pass through perimeter filtering devices (routers, firewalls, etc) to limit the possible points of attack. There are many benefits to this method including the prevention of unauthorized systems communicating outside the State's network. If a procedure is implemented that explicitly denies all traffic a greater amount of control and understanding can be gained about the State's network. A change control system should include a method of tracking, the purpose of the traffic rule, and an authorization mechanism to provide for checks and balances.

4. Web Server Vulnerabilities

The second highest number of vulnerabilities was associated with port 80, which is the default port for HTTP traffic. This would be expected due to the high percentage of Web servers on the

Internet. Patching the applications and adjusting the configurations can mitigate these vulnerabilities. The HTTP and HTTPS protocols were also identified on many other ports, which is not a vulnerability, but may indicate a situation where the service is unauthorized and is trying to avoid detection by running on a non-standard port.

5. Internet Relay Chat

Ten (10) hosts where found to be running IRC. This chatting protocol is associated with hackers and illegal software distributors. IRC consumes bandwidth and does not have a typical business use. The State expressed an interest in identifying hosts running this protocol as it has been discovered in the past on hosts that have been compromised.

6. MS-SQL Port 1433

Twenty-six (26) hosts were found with port 1433 open, and this indicates that an instance of Microsoft's SQL database server is running on these hosts. The recent SQL Slammer worm caused disruptions on the Internet due to un-patched servers with this port open to the outside world. There is typically no reason to offer this service to the external network and this port should be blocked.

7. TFTP Port 69

Ten (10) hosts were found to be running Trivial File Transfer Protocol. TFTP can be dangerous to systems because there is no authentication mechanism in place. If a host is running TFTP an attack only needs a client to place or retrieve files from a system. This protocol should be removed or blocked.

8. Outdated operating systems

Several hosts have been identified running MS-Windows NT that is at the end of life for Microsoft. Several vulnerabilities have been identified on hosts running this operating system, some of which can not be addressed by normal patching. The applications running on these hosts are in danger of being compromised. The best approach would be to upgrade or replace the systems that are running older operating systems.

One agency in particular has hosts with outdated operating systems. Through the course of Phase II testing, several issues were uncovered with the web server supporting this agency. The agency was notified and chose not to resolve the issues as they are migrating their platform to the Nebraska Online facility.

Several versions of the Linux kernel were also identified. Older versions of the open-source operating systems have known flaws, which can lead to the compromise of the system.

9. Scanning traffic blocked

On a few occasions traffic from the Omni Tech Corporation facility was blocked by the IS staff. The amount of traffic being generated into the logging system was slowing down the network to the point that people were complaining. The choice was made to block the traffic. Unfortunately, no notification was made to Omni Tech Corporation and it took several days to clear up the issue. A more suitable resolution would have been not to log the traffic from Omni Tech Corporation and allow testing to continue. In the future if testing on a large scale will be performed a notification method should be established and the proper log file configuration should be agreed upon before such testing begins.

10. Other High Risk Vulnerabilities

A summary of high-risk vulnerabilities and the frequency of each includes:

High Risk Vulnerability	Total Servers	Total Agencies
Active SNMP Agent	79	12
Apache HTTP Server Chunked Encoding Buffer Overflow	8	6
BIND SIG Cached Resource Record Overflow	3	3
FormMail CGI	1	1
HTTP DELETE Method Allowed	1	1
HTTP PUT Method allowed	1	1
Imapd Buffer Overflow	2	2
IPSSWITCH IMail File Attachment	1	1
ISC Bind 8 Transaction Signature Buffer Overflow	1	1
Lotus Domino Authentication Bypass	1	1
Microsoft ADCTEST.ASP Sample File	3	3
Microsoft SQL Server Weak Authentication	11	7
Multiple Vendor BIND NXT Overflow	1	1
NFS Export is Writeable	1	1
NFS Mountable Volume List	1	1
O'Reilly WebSite 'webfind.exe' Buffer Overflow	2	2
O'Reilly WebSite GET Buffer Overflow	2	2
Piranha Linux Virtual Server Default Password	1	1
RDS/IIS	5	5
Rexec Service is Running	2	2
Rsh Service is Running	1	1
SSH CRC-32 Compensation Attack Detector	1	1
TFTPD32 Arbitrary File Download/Upload	2	2

APPENDIX C

LIST OF AGENCY REPORTS FOR PHASE II AND PHASE III

(For access to the reports, contact Doug Hahn at IMServices – 471-9578.)

Agency	Phase II	Phase III
Coordinating Commission for Higher Education	X	
Crime Commission		X
Department of Correctional Services	X	X
Department of Economic Development	X	X
Department of Education	X	X
Department of Environmental Quality	X	X
Department of Health and Human Services	X	X
Department of Insurance	X	
Department of Labor	X	X
Department of Motor Vehicles	X	
Department of Natural Resources	X	X
Department of Property Assessment and Taxation	X	
Department of Revenue	X	X
Department of Roads	X	X
Division of Communications	X	X
Game and Parks Commission	X	
Information Management Services Division	X	X
Legislative Council	X	X
Library Commission	X	X
NDE – Assistive Technology Partnership	X	
NDE – Developmental Disability	X	
Nebraska Information System	X	
Nebraska Online		X
Public Employees Retirement Systems	X	X
Secretary of State	X	X
State College System	X	
State Personnel	X	
State Surveyor	X	
State Treasurer	X	
Workers Compensation Board	X	